SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

AUTONOMIC SYSTEM FOR SELECTIVE ADMINISTRATION ISOLATION OF A SECURE REMOTE MANAGEMENT OF SYSTEMS IN A COMPUTER NETWORK

Field of the Invention

[0001] The present invention relates generally to management systems and more particularly to an autonomic system for selective administration isolation for more secure remote management of systems in a computer network.

Background of the Invention

[0002] Large-scale computer networks provide many types of services and applications, where typically there are one or more servers accessible by multiple end-users/clients. One consideration of computer networks is the utilization of an authentication protocol or mechanism to ensure that only authorized operations/access for a particular user occur. A further consideration is the establishment of system administrator(s) who are responsible for managing the computer network. Often management of the network occurs through remote management. Normally, remote management is done in a peer-to-peer arrangement, such as a remote console takeover of a client. With such a takeover, the system administrator has access to the client's operating system log-on information/security credentials.

[0003] The broad access to a client's system presents an opportunity for security

breaches in a network, e.g., by a rogue acting as an administrator to infiltrate the network. Accordingly, what is needed is an approach for system administration of remote clients in a computer network that provides an administrator enough access to perform remote operations, both attended and unattended by a user of the remote client, without providing so much access that the security of the client or privacy of its user is compromised. The present invention addresses such a need.

Summary of Invention

[0004] An autonomic system for selective administration isolation for more secure remote management in a computer network is disclosed. The aspects include isolating administrative access to managed client systems in a computer network via a data center, and utilizing the data center to control remote initiation of services in the managed client systems by an administrative system.

[0005] Through the present invention, peer-to-peer management is avoided through the inclusion of a trusted third party in the form of a data center. User data privacy can be enforced and system configuration can be limited to administrator control, which are both accomplished under the enforcement of the data center. These and other advantages will become readily apparent from the following detailed description and accompanying drawings.

Brief Description of Drawings

[0006] Figure 1 illustrates a diagram of a system for selective administration isolation in accordance with a preferred embodiment of the present invention.

[0007] Figure 2 illustrates a block flow diagram of selective administration isolation in accordance with a preferred embodiment of the present invention.

Detailed Description

[0008] The present invention relates generally to management systems and more particularly to an autonomic system for selective administration isolation for more secure remote management of systems in a computer network. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements.

Various modifications to the preferred embodiment and the generic principles and features described herein will be readily apparent to those skilled in the art. Thus, the present invention is not intended to be limited to the embodiment shown but is to be accorded the widest scope consistent with the principles and features described herein.

[0009] Referring to Figure 1, a computer network system, in accordance with a preferred embodiment of the present invention, is illustrated. It should be appreciated that although the network system 10 is illustrated as being on a world wide web- based network 12, i.e., the Internet, this is illustrative and not restrictive of the arrangement for the network 10. Included in the network system 10 are one or more service administrator systems 14, e.g., a help center terminal for managing client systems 16, 16a, 16b or 16c, e.g., personal computers. Further included is a data center 18 that acts as a trusted third party for all accesses by the administrator 14 to any of the managed client systems 16, 16a, 16b or 16c, as described with reference to the block flow diagram of Figure 2. The data center 18 suitably is provided on a computer system as part of a utility backbone for the network, e.g., as part of an e-business service utility to support Internet marketplace functionality, including, for example, services for trusted shopping, intelligent content management, databases, support routing, etc.

[0010] With reference to Figure 2, in order to provide the actions of a trusted third party by the data center 18 for all administrator 14 accesses to managed clients 16, 16a, 16b or 16c administrator personnel are first authenticated to their respective computer systems (step 20). The authentication preferably includes the use of an embedded security chip as part of the hardware of the administrator systems to uniquely identify the system and biometric/badge authentication of its user, e.g., fingerprint touchpad to read the fingerprint of the administrator combined with the input of a proximity badge identifying the administrator. Once authenticated to their machine, the administrator systems are further authenticated to the data center 18 (step 22). Preferably, the communications between the administrators and the data center 18 are secured based on PKI (public key infrastructure) with VPN (virtual public network) and SSL (secure socket layer) protocol machine authentication, as is well understood by those skilled in the art.

[0011] Commands from the administrator systems 14, such as to do a back-up operation, restore files, etc. on a client system, are then transmitted to the data center 18 and verified by digital signature (step 24). The data center 18 then determines whether the administrator is allowed to perform the commands based on pre-existing data contained therein relating administrators and their approved capabilities (step 26). When the administrator does have approval to perform the command, the data center 18 issues an appropriately signed, trusted message to the intended client 16, 16a, 16b or 16c (step 28). In a preferred embodiment, the data center 18 communicates with an agent in the client system 16, 16a, 16b or 16c using a user ID and password known only to the data center 18 and agent and inaccessible to the user of the client system 16. The client system 16, 16a, 16b or 16c then validates the signature of the received message as being from the trusted third party (not the admin directly and decrypts the message via the agent (step 30). Thus, the system administrators never have direct access to the client's operating system log-ons or security credentials, even though working through the data center, the administrators are able to act as if they were a local administrator.

[0012] With the inclusion of the data center in accordance with the present invention, a control chain exists which allows services to be efficiently and securely run on any given client PC when remotely initiated only by the data center itself. Neither the administrator nor the user can take on the capabilities of the trusted third party, the data center. User data privacy can be enforced and system configuration can be limited to administrator control, which are both accomplished under the enforcement of the data center. The data center can remotely control a PC, under request of an authenticated administrator, and when necessary, on behalf of a user. Further, the ability to uniquely tie the administrator to a computer system as part of the authentication reduces the opportunity for unauthorized administrative use when that computer system is not present. In this manner, a high level of accountability exists, since actions of the administrator are directly related to a piece of equipment for which the administrator is already accountable as a business asset.

[0013] From the foregoing, it will be observed that numerous variations and modifications may be effected without departing from the spirit and scope of the novel concept of the invention. It is to be understood that no limitation with respect to

the specific methods and apparatus illustrated herein is intended or should be inferred. It is, of course, intended to cover by the appended claims all such modifications as fall within the scope of the claims.